On Point Sets in Vector Spaces over Finite Fields That Determine Only Acute Angle Triangles

Igor E. Shparlinski
Department of Computing
Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

Abstract

For three points $\mathbf{u}$, $\mathbf{v}$ and $\mathbf{w}$ in the n-dimensional space $\mathbb{F}_q^n$ over the finite field $\mathbb{F}_q$ of q elements we give a natural interpretation of an acute angle triangle defined by this points. We obtain an upper bound on the size of a set $\mathcal{Z}$ such that all triples of distinct points $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathcal{Z}$ define acute angle triangles. A similar question in the real space $\mathcal{R}^n$ dates back to P. Erdős and has been studied by several authors.

2000 Mathematics Subject Classification: 11T30, 52C10

1 Introduction

Recent remarkable results of Bourgain, Katz and Tao [3] on the sum-product problem in finite fields have stimulated a series of studies of finite field analogues of classical combinatorial and discrete geometry problems, see [2, 4, 5, 6, 8, 9, 10, 11, 12, 13, 14, 16, 19, 20, 21, 22, 23] and references therein.

Here we extend the scope of such problems and consider the question about the largest cardinality of a set of points in the n-dimensional space over a finite field such that every triples of distinct points of this set defines

an acute angle triangle. We note that a similar question in the Euclidean space $\mathcal{R}^n$ dates back to P. Erdős and has been studied by several authors, see [1].

Certainly the notion of an acute triangle (or angle) is not immediately obvious in vector spaces over finite fields. Here we use the "rational" interpretation of trigonometry invented by Wildberger [24] to extend this notion to finite fields.

To motivate our definition, we note that in the triangle defined by three distinct vectors $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{R}^n$, the vertex at $\mathbf{u}$ has an acute angle if and only if

$$\|\mathbf{u}-\mathbf{v}\|^2 + \|\mathbf{u}-\mathbf{w}\|^2 - \|\mathbf{v}-\mathbf{w}\|^2 > 0,$$

where $\|\mathbf{x}\|$ is the Euclidean norm of $\mathbf{x} \in \mathbb{R}^n$.

We now identify positive elements of a finite field $\mathbb{F}_q$ of q elements with quadratic residues in $\mathbb{F}_q$ and say that in the triangle defined by three distinct vectors

$$\mathbf{u} = (u_1, \ldots, u_n),\ \mathbf{v} = (v_1, \ldots, v_n),\ \mathbf{w} = (w_1, \ldots, w_n) \in \mathbb{F}_q^n$$

that the vertex at $\mathbf{u}$ has an acute angle if any only if

$$\Delta(\mathbf{u}, \mathbf{v}, \mathbf{w}) = \sum_{i=1}^{n} \left((u_i - v_i)^2 + (u_i - w_i)^2 - (v_i - w_i)^2\right)$$

is a quadratic residue in $\mathbb{F}_q$.

Since in the field of even characteristic we always have $\Delta(\mathbf{u}, \mathbf{v}, \mathbf{w}) = 0$, this definition makes sense only if q is odd.

We also remark that

$$\begin{aligned} \Delta(\mathbf{u}, \mathbf{v}, \mathbf{w}) = 2\sum_{i=1}^{n} \left(u_i^2 - u_i v_i - u_i w_i + v_i w_i\right) = \\ = 2\left(\mathbf{u}\cdot\mathbf{u} - \mathbf{u}\cdot\mathbf{v} - \mathbf{u}\cdot\mathbf{w} + \mathbf{v}\cdot\mathbf{w}\right) = 2(\mathbf{u}-\mathbf{v})\cdot(\mathbf{u}-\mathbf{w}), \end{aligned} \tag{1}$$

where $\mathbf{a}\cdot\mathbf{b}$ denotes the inner product of $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$. Thus, if q is odd then $\Delta(\mathbf{u}, \mathbf{v}, \mathbf{w}) = 0$ if an only if $(\mathbf{u}-\mathbf{v})\cdot(\mathbf{u}-\mathbf{w}) = 0$, which correspond to the orthogonality at $\mathbf{u}$ and thus to the Pythagoras theorem.

Let $N(n, q)$ be the largest possible cardinality of a set $\mathcal{Z} \subseteq \mathbb{F}_q$ such that all triples of distinct points $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathcal{Z}$ define acute angle triangles.

We remark that [8, Theorem 1.1] immediately implies that

$$N(n, q) = O(q^{(n+1)/2}), \tag{2}$$

where the implied constant depends only on n. In general, we do not know how to improve this bound. However for $n = 2$ we obtain a stronger estimate.

Theorem 1. *For a sufficiently large odd q,*

$$N(2, q) \le 2q^{4/3}.$$

2 Additive Character Sums

Let Ψ be the set of all additive characters of $\mathbb{F}_q$ and let $\Psi^* \subset \Psi$ be the set of all nonprincipal characters, see [15, Section 11.1] for basic properties of additive characters. In particular, we also recall the identity

$$\sum_{\psi \in \Psi} \psi(z) = \begin{cases} q, & \text{if } z = 0, \\ 0, & \text{otherwise}, \end{cases} \tag{3}$$

see [15, Section 11.1].

For an additive character $\psi \in \Psi$ and $\alpha \in \mathbb{F}_q$, we define the Gauss sum

$$G_\psi(\alpha) = \sum_{z \in \mathbb{F}_q} \psi(\alpha z^2) = \sum_{z \in \mathbb{F}_q} \chi(z)\psi(\alpha z)\chi(\alpha) \sum_{z \in \mathbb{F}_q} \chi(z)\psi(z) = \chi(\alpha) G_\psi(1),$$

where χ is the quadratic character in $\mathbb{F}_q$ (which exists since q is odd), and recall that

$$|G_\psi| = q^{1/2}, \tag{4}$$

for $\psi \in \Psi^*$ and $\alpha \in \mathbb{F}_q^*$, see [15, Proposition 11.5].

Finally, given a set $\mathcal{Z} \subseteq \mathbb{F}_q^n$, we define the triple character sum

$$S_\psi(\mathcal{Z}) = \sum_{\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathcal{Z}} \psi\left(\Delta(\mathbf{u}, \mathbf{v}, \mathbf{w})\right).$$

Although we use our result on $S_\psi(\mathcal{Z})$ only in the case of $n = 2$, here we present it in full generality as it may have some other applications.

Lemma 2. *For any $\psi \in \Psi^*$ and a set $\mathcal{Z} \subseteq \mathbb{F}_q^n$, we have*

$$|S_\psi(\mathcal{Z})|^2 \leq \#\mathcal{Z} q^n \sum_{\substack{\mathbf{v},\mathbf{w},\mathbf{x},\mathbf{y} \in \mathcal{Z} \\ \mathbf{v}+\mathbf{w}=\mathbf{x}+\mathbf{y}}} \psi\left(2\left(\mathbf{v}\cdot\mathbf{w} - \mathbf{x}\cdot\mathbf{y}\right)\right).$$

Proof. We have

$$|S_\psi(\mathcal{Z})| \leq \sum_{\mathbf{u}\in\mathcal{Z}} \left| \sum_{\mathbf{v},\mathbf{w}\in\mathcal{Z}} \psi\left(\Delta(\mathbf{u},\mathbf{v},\mathbf{w})\right) \right|.$$

Hence, recalling (1), we derive

$$|S_\psi(\mathcal{Z})| \leq \sum_{\mathbf{u}\in\mathcal{Z}} \left| \sum_{\mathbf{v},\mathbf{w}\in\mathcal{Z}} \psi\left(-2\left(\mathbf{u}\cdot(\mathbf{v}+\mathbf{w}) - \mathbf{v}\cdot\mathbf{w}\right)\right) \right|.$$

Note that since $\psi(-z) = \overline{\psi(z)}$, we can replace -2 with 2. By the Cauchy inequality

$$\begin{aligned}
|S_\psi(\mathcal{Z})|^2 &\leq \#\mathcal{Z} \sum_{\mathbf{u}\in\mathcal{Z}} \left| \sum_{\mathbf{v},\mathbf{w}\in\mathcal{Z}} \psi\left(2\left(\mathbf{u}\cdot(\mathbf{v}+\mathbf{w}) - \mathbf{v}\cdot\mathbf{w}\right)\right) \right|^2 \\
&\leq \#\mathcal{Z} \sum_{\mathbf{u}\in\mathbb{F}_q^n} \left| \sum_{\mathbf{v},\mathbf{w}\in\mathcal{Z}} \psi\left(2\left(\mathbf{u}\cdot(\mathbf{v}+\mathbf{w}) - \mathbf{v}\cdot\mathbf{w}\right)\right) \right|^2 \\
&= \#\mathcal{Z} \sum_{\mathbf{u}\in\mathbb{F}_q^n} \sum_{\mathbf{v},\mathbf{w},\mathbf{x},\mathbf{y}\in\mathcal{Z}} \psi\left(2\left(\mathbf{u}\cdot(\mathbf{v}+\mathbf{w}-\mathbf{x}-\mathbf{y}) - \mathbf{v}\cdot\mathbf{w} + \mathbf{x}\cdot\mathbf{y}\right)\right) \\
&= \#\mathcal{Z} \sum_{\mathbf{v},\mathbf{w},\mathbf{x},\mathbf{y}\in\mathcal{Z}} \psi\left(2\left(\mathbf{x}\cdot\mathbf{y} - \mathbf{v}\cdot\mathbf{w}\right)\right) \sum_{\mathbf{u}\in\mathbb{F}_q^n} \psi\left(2\mathbf{u}\cdot(\mathbf{v}+\mathbf{w}-\mathbf{x}-\mathbf{y})\right).
\end{aligned}$$

Finally, changing the order of summation, and replacing $2\mathbf{u}$ with $\mathbf{u}$, we obtain

$$|S_\psi(\mathcal{Z})|^2 \leq \mathcal{Z} \sum_{\mathbf{v},\mathbf{w},\mathbf{x},\mathbf{y}\in\mathcal{Z}} \psi\left(2\left(\mathbf{x}\cdot\mathbf{y} - \mathbf{v}\cdot\mathbf{w}\right)\right) \sum_{\mathbf{u}\in\mathbb{F}_q^n} \psi\left(\mathbf{u}\cdot(\mathbf{v}+\mathbf{w}-\mathbf{x}-\mathbf{y})\right).$$

By the orthogonality property of additive characters (3), we see that the inner sum vanishes if and only if

$$\mathbf{v}+\mathbf{w}-\mathbf{x}-\mathbf{y} = 0$$

in which case it equals q^n. Now renaming the variables $(\mathbf{v},\mathbf{w}) \leftrightarrow (\mathbf{x},\mathbf{y})$, we conclude the proof. $\square$

3 Proof of Theorem 1

Assume that for set $\mathcal{Z} \subseteq \mathbb{F}_q^2$ all triples of distinct vectors $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathcal{Z}$ define acute angle triangles. Fix an arbitrary quadratic non-residue $\alpha \in \mathbb{F}_q$. Then we see that the equation

$$\Delta(\mathbf{u}, \mathbf{v}, \mathbf{w}) = \alpha z^2, \qquad \mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathcal{Z},\ z \in \mathbb{F}_q,$$

has at most

$$T \le (\#\mathcal{Z})^2 \tag{5}$$

solutions (which come only from the triples $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathcal{Z}$ with $\Delta(\mathbf{u}, \mathbf{v}, \mathbf{w}) = 0$, that is, when $\mathbf{u} = \mathbf{v}$ or $\mathbf{u} = \mathbf{w}$).

On the other hand, from the orthogonality property of characters (3), we obtain

$$T = \sum_{\mathbf{u},\mathbf{v},\mathbf{w} \in \mathcal{Z}} \sum_{z \in \mathbb{F}_q} \frac{1}{q} \sum_{\psi \in \Psi} \psi\left(\Delta(\mathbf{u}, \mathbf{v}, \mathbf{w}) - \alpha z^2\right) = \frac{1}{q} \sum_{\psi \in \Psi} G_\psi(-\alpha) S_\psi(\mathcal{Z}).$$

The term corresponding to the principal character $\psi = \psi_0$ is equal to $(\#\mathcal{Z})^3$. Thus, recalling (4), we obtain

$$\left|T - (\#\mathcal{Z})^3\right| \le q^{-1/2} R, \tag{6}$$

where

$$R = \sum_{\psi \in \Psi^*} |S_\psi(\mathcal{Z})|.$$

Now, by the Cauchy inequality

$$R^2 = q \sum_{\psi \in \Psi^*} |S_\psi(\mathcal{Z})|^2.$$

Thus using Lemma 2 and then exteding the summation to all $\psi \in \Psi$, we deduce

$$R^2 \le \#\mathcal{Z} q^3 \sum_{\psi \in \Psi} \sum_{\substack{\mathbf{v},\mathbf{w},\mathbf{x},\mathbf{y} \in \mathcal{Z} \\ \mathbf{v}+\mathbf{w}=\mathbf{x}+\mathbf{y}}} \psi\left(2\left(\mathbf{v} \cdot \mathbf{w} - \mathbf{x} \cdot \mathbf{y}\right)\right).$$

Changing the order of summation and using (3) again, we obtain

$$R^2 = \#\mathcal{Z} q^3 \sum_{\substack{\mathbf{v},\mathbf{w},\mathbf{x},\mathbf{y} \in \mathcal{Z} \\ \mathbf{v}+\mathbf{w}=\mathbf{x}+\mathbf{y}}} \sum_{\psi \in \Psi} \psi\left(2\left(\mathbf{v} \cdot \mathbf{w} - \mathbf{x} \cdot \mathbf{y}\right)\right) = \#\mathcal{Z} q^4 W, \tag{7}$$

where W is the number of solutions to the system of equations

$$\mathbf{v} + \mathbf{w} = \mathbf{x} + \mathbf{y} \qquad \text{and} \qquad \mathbf{v} \cdot \mathbf{w} = \mathbf{x} \cdot \mathbf{y}$$

in $\mathbf{v}, \mathbf{w}, \mathbf{x}, \mathbf{y} \in \mathcal{Z}$, which is the same as the number of solutions to the equation

$$\mathbf{v} \cdot \mathbf{w} = \mathbf{x} \cdot (\mathbf{v} + \mathbf{w} - \mathbf{x})$$

in $\mathbf{v}, \mathbf{w}, \mathbf{x} \in \mathcal{Z}$. Clearly, when $\mathbf{v}, \mathbf{w}$ and one component of $\mathbf{x}$ are fixed, we obtain a nontrivial quadratic equation over $\mathbb{F}_q$ for the other component of $\mathbf{x}$. Therefore

$$W \le 2\,(\#\mathcal{Z})^2\,q.$$

Substituting in (7), we obtain

$$R^2 \le 2\,(\#\mathcal{Z})^3\,q^5.$$

In turn, inserting this estimate in (6) yields

$$\left|T - (\#\mathcal{Z})^3\right| \le \sqrt{2}\,(\#\mathcal{Z})^{3/2}\,q^2. \tag{8}$$

If $\#\mathcal{Z} < 2q^{4/3}$ then there is nothing to proof. Otherwise,

$$\sqrt{2}\,(\#\mathcal{Z})^{3/2}\,q^2 \le \frac{1}{2}\,(\#\mathcal{Z})^3$$

thus, by (8) we obtain

$$T \ge \frac{1}{2}\,(\#\mathcal{Z})^3$$

which contradicts to (5), provided that q is large enough.

4 Remarks

Unfortunately the method of this paper, although works for any n, leads to a bound which is that same as (2) for $n = 3$ and is even weaker than (2) for $n \ge 4$.

Furthermore, using the bound

$$|S_\psi(\mathcal{Z})| \le (\#\mathcal{Z})^2\,q^{n/2}$$

(which is immediate from Lemma 2) in the argument of the proof of Theorem 1 one can recover the bound (2), but it does not seem to give anything stronger that this.

An alternative way to estimating $N(n,q)$ is via bounds of quadratic character sums

$$T_\chi(\mathcal{Z}) = \sum_{\mathbf{u},\mathbf{v},\mathbf{w}\in\mathcal{Z}} \chi\left(\Delta(\mathbf{u},\mathbf{v},\mathbf{w})\right).$$

Using the same approach (via Cauchy inequality and extending summation over $\mathbf{u}\in\mathcal{Z}$ to the full space $\mathbb{F}_q^n$) as in the proof of Lemma 2, we obtain

$$|T_\chi(\mathcal{Z})|^2 = \#\mathcal{Z} \sum_{\mathbf{v},\mathbf{w},\mathbf{x},\mathbf{y}\in\mathcal{Z}} \sum_{\mathbf{u}\in\mathbb{F}_q^n} \chi\left(\Delta(\mathbf{u},\mathbf{v},\mathbf{w})\Delta(\mathbf{u},\mathbf{x},\mathbf{y})\right).$$

It is natural to conjecture that the inner sums admits a square root estimate and thus is $O(q^{n/2})$ unless $(\mathbf{v},\mathbf{w})$ is a permutation of $(\mathbf{x},\mathbf{y})$. One can derive that $N(n,q) = O(q^{n/2})$ from such a hypothetical bound. Unfortunately the highest form of the polynomial

$$F_{\mathbf{v},\mathbf{w},\mathbf{x},\mathbf{y}}(\mathbf{U}) = \Delta(\mathbf{U},\mathbf{v},\mathbf{w})\Delta(\mathbf{U},\mathbf{x},\mathbf{y}) \in \mathbb{F}[\mathbf{U}]$$

is singular, so known analogues of the Deligne bound for multivariate character sums, see [17, 18], do not apply.

We recall that in $\mathbb{R}^n$, the largest number of vectors such that each three of them define an acute angle triangle is bounded by a function of n, see [1]. Although our bounds seem to be much higher that the true order of magnitude of $N(n,q)$, we observe that $\limsup_{p\to\infty} N(n,p) = \infty$. Indeed, by the result of Graham and Ringrose [7], there is an absolute constant $C > 0$ such that for infinitely many primes p all nonnegative integers $z \le C \log p \log\log\log p$ are quadratic residues modulo p. Thus, for each such p and an appropriate constant c, for the set $\mathcal{Z} \subseteq \mathbb{F}_p$ formed by vectors with conponents in the interval $[1, c\sqrt{\log p \log\log\log p}]$ we have

$$1 \le \Delta(\mathbf{u},\mathbf{v},\mathbf{w}) \le C \log p \log\log\log p$$

for any pairwise distinct $\mathbf{u},\mathbf{v},\mathbf{w} \in \mathcal{Z}$ and thus $\Delta(\mathbf{u},\mathbf{v},\mathbf{w})$ is a quadratic residue. This implies

$$\limsup_{p\to\infty} \frac{N(n,p)}{(\log p \log\log\log p)^{n/2}} > 0.$$

Acknowledgements

The authors is grateful to Norman Wildberger for his suggestion of an $\mathbb{F}_q$-interpretation of acute angle triangles, which has been used here.

The authors would also like to thank Nick Katz for a useful discussion of some issues related to possible estimates of the quadratic character sums $T_\chi(\mathcal{Z})$.

During the preparation of this paper, the author was supported in part by ARC grant DP0556431.

References

[1] E. Ackerman and Oren Ben-Zwi, 'On sets of points that determine only acute angles, *European J. Combin.*, **30** (2009) 908–910.

[2] J. Bourgain and M. Z. Garaev, 'On a variant of sum-product estimates and explicit exponential sum bounds in prime fields', *Math. Proc. Cambr. Phil. Soc.*, **146** (2008), 1–21.

[3] J. Bourgain, N. Katz and T. Tao, 'A sum product estimate in finite fields and Applications', *Geom. Funct. Analysis*, **14** (2004), 27–57.

[4] D. Covert, D. Hart, A. Iosevich, D. Koh and M. Rudnev, 'Generalized incidence theorems, homogeneous forms and sum-product estimates in finite fields', *European J. Combin.*, (to appear).

[5] Z. Dvir, 'On the size of Kakeya sets in finite fields', *J. Amer. Math. Soc.* (to appear).

[6] M. Z. Garaev, 'The sum-product estimate for large subsets of prime fields', *Proc. Amerc. Math. Soc.*, **136** (2008), 2735–2739.

[7] S. W. Graham and C. J. Ringrose, 'Lower bounds for least quadratic nonresidues', *Analytic Number Theory, Allerton Park 1989*, Progress in Mathematics, vol. 85, Birkhäuser, Basel, 1990, 269–309.

[8] D. Hart and A. Iosevich, 'Ubiquity of simplices in subsets of vector spaces over finite fields', *Analysis Mathematica*, **34** (2007), 29–38.

[9] D. Hart, A. Iosevich, D. Koh and M. Rudnev, 'Averages over hyperplanes, sum-product theory in finite fields', *Trans. Amer. Math. Soc.* (to appear).

[10] D. Hart, A. Iosevich and J. Solymosi, 'Sums and products in finite fields via Kloosterman sums', *Intern. Math. Res. Notices*, **2007** (2007), Article ID rnm007, 1–14.

[11] A. Iosevich and D. Koh, 'ErdősFalconer distance problem, exponential sums, and Fourier analytic approach to incidence theorems in vector spaces over finite fields', *SIAM J. Disc. Math.*, **23** (2008), 123–135.

[12] A. Iosevich and M. Rudnev, 'Erdős distance problem in vector spaces over finite fields', *Trans. Amer. Math. Soc.*, **359** (2007), 6127–6142.

[13] A. Iosevich, I. E. Shparlinski and M. Xiong, 'Sets with integral distances in finite fields', *Trans. Amer. Math. Soc.* (to appear).

[14] A. Iosevich and S. Senger, 'Orthogonal systems in vector spaces over finite fields', *The Electronic J. Combin.*, **15** (2008), Article R151.

[15] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.

[16] N. H. Katz and C.-Y. Shen, 'Garaev's inequality in finite fields not of prime order', *J. Anal. Combin.*, **3** (2008), Article 3.

[17] N. M. Katz, 'Estimates for nonsingular multiplicative character sums', *Intern. Math. Res. Notices*, **2002** (2002), 333–349.

[18] G. I. Perel?muter, 'Estimation of a multiple sum with the Legendre symbol', *Mat. Zametki*, **18** (1975), 421–427 (in Russian).

[19] C.-Y. Shen, 'An extension of Bourgain and Garaev's sum-product estimates', *Acta Arith.*, **135** (2008), 351–256.

[20] L. A. Vinh, 'Explicit Ramsey graphs and Erdős distance problem over finite Euclidean and non-Euclidean spaces', *Electronic J. Combin.*, **15** (2008), Aricle R5.

[21] L. A. Vinh, 'On the number of orthogonal systems in vector spaces over finite fields', *Electronic J. Combin.*, **15** (2008), Aricle N32.

[22] L. A. Vinh, 'On a Furstenberg-Katznelson-Weiss type theorem over finite fields', *Annals Combin.*, (to appear).

[23] L. A. Vinh, 'Szemeredi-Trotter type theorem and sum-product estimate in finite fields', *European J. Combin.*, (to appear).

[24] N. J. Wildberger, *Divine proportions: Rational trigonometry to universal geometry*, Wild Egg Books, Sydney, 2005.